Риск-модели и критерии информационного противоборства в социальных сетях

Назаров Алексей Николаевич; Московский физико-технический институт; 141700, Российская Федерация, Московская область, г.Долгопрудный, Институтский пер., 9; профессор, доктор технических наук; a.nazarov06@bk.ru

Галушкин Александр Иванович; Московский физико-технический институт; 141700, Российская Федерация, Московская область, г.Долгопрудный, Институтский пер., 9; заместитель заведующего кафедрой, профессор; доктор технических наук; neurocomputer@yandex.ru

Сычев Артем Константинович; ООО «СмартТек»; адрес: 119454, Москва, ул.Коштоянца, 21а; старший научный сотрудник; sychev_a_k@mail.ru

Аннотация.

В настоящее время социальные медиа (СМ) – социальные сети, блоги и микроблоги, геосоциальные сервисы, фотохостинги и видеохостинги – являются динамическими источниками разнородной информации, отражающей различные процессы, протекающие в реальном обществе. Актуальность социальных сетей растёт в связи с использованием их возможностей как средства привлечения информационных, интеллектуальных, финансовых ресурсов в экономике, политике, региональном и локальном развитии.

Под «информационным противоборством в сети Интернет» следует понимать соперничество политических акторов посредством использования специальных информационно-технических ресурсов Интернета для воздействия на информационную среду противостоящей стороны, влияние на ее аудиторию и различные сферы политико-властных отношений с целью установления контроля над источниками виртуальных и электронных стратегических ресурсов актора-оппонента и достижения информационного превосходства. Другими словами актор-агрессор для целей информационного превосходства над актором-защитником предпринимает информационную атаку против объекта в web-пространстве, успех которой является победой, в смысле достижения целей информационного превосходства.

При использовании информационного воздействия основную роль играет личность как элемент общения, как участник коллективной деятельности, как член многочисленных малых и больших групп и аудиторий. Однако не менее важную роль играют методы информационного управления малыми коллективами, большими социальными общностями и массовыми процессами.

По сути, граждане становятся обширной наземной социальной сенсорной сетью, отражая структуру общества в режиме реального времени почти в каждом уголке мира, а скорость и объем этой сенсорной сети, особенно в условиях «Интернета везде» растет с каждым днем.

Скрытое информационное-психологическое воздействие на население в социальных сетях используют с целью решения следующих задач: информационное влияние на отдельные личности, социальные и другие группы, общество в целом; информационное влияние на целесообразность и оперативность управленческих решений руководством страны и силовых ведомств, принимаемых на основе этой информации; манипулирование общественным мнением при помощи средств массовой информации и, в особенности, посредством сервисов социальных сетей; дискредитация неугодных лидеров; автоматизированного распространения информации в крупных социальных сетях и организации информационной поддержки мероприятий по подготовленным сценариям воздействия а заданную массовую аудиторию социальных сетей.

Таким образом, анализируя активность интернет-сообществ, посредством проблемно-ориентированных систем мониторинга, можно, например, выявить наличие социального стресса (напряженности), определить его степень и направленность, предсказать социальные волнения, способные вылиться в неконтролируемые массовые протестные акции.

На основе логического вероятностного подхода, предлагается модель риска для успешных атак на социальные медиа в Интернете с точки зрения информационной войны. Сформулированы и исследованы возможные риск-критерии для принятия решений, направленных на достижение целей информационного противоборства. Для разработанных критериев предлагаются структура и алгоритмической основы системы мониторинга социальных сетей для кластера Hadoop.

Ключевые слова: информационное противоборство, полином, риск-модель, риск-критерий, актор, социальная сеть, мониторинг, функция защиты, кластер Hadoop, демон

Литература

[1] A. N. Nazarov, “Estimation of information safety level of modern infocommunication networks on basis of logic-probability approach,” Automation and Remote Control, July 2007, Volume 68 Issue 7, 2007, pp. 1165-1176, doi: 10.1134/S0005117907070053.

[2] A. N. Nazarov, “LOGICAL-AND-PROBABILISTIC MODEL FOR ESTIMATING THE LEVEL OF INFORMATION SECURITY OF MODERN INFORMATION AND COMMUNICATION NETWORKS,”

Telecommunications and Radio Engineering, USA, 2010, Vol. 69, № 16, pp. 1453-1463, doi: 10.1615/TelecomRadEng.v**69**.i**16**.60.

[3] Nazarov A. 'Botnet tracking and global threat intelligence - behavior approaches to identifying distributed botnets' paper presented at the IEEE / Collection of proceedings of the *Cybersecurity Summit (WCS), 2012 Third Worldwide, New Dehli, 30-31 Oct. 2012.* http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6780878&newsearch=true&queryText=Botnet%20tracking%20and%20global%20threat%20intelligence%20-%20behavior%20approaches%20to%20identifying%20distributed%20botnets

[4] Осипов Г.С. Методы и программные средства для получения оценок уровня социального стресса на основе анализа информации Интернет. Режим доступа: https://www.gkpromtech.ru/material/view?id=27. Дата обращения: 10.02.2015.

[5] Волков Д.А., Назаров А.Н., Назаров М.А. Глобальная угроза – Теневой Интернет// Сборник ежегодных научных трудов Международной конференции «Управление развитием крупномасштабных систем» (MLSD'2014), М.: ИПУ РАН.-2014 г.- С.452-459.

Risk models and criteria of information confrontation in social networks

Nazarov Alexey Nikolaevich; Moscow Institute of Physics and Technology; 9 Institutskiy per., Dolgoprudny, Moscow Region, 141700, Russian Federation; Professor, Doctor of Technical Sciences; a.nazarov06@bk.ru

Galushkin Alexander Ivanovich; Moscow Institute of Physics and Technology; 9 Institutskiy per., Dolgoprudny, Moscow Region, 141700, Russian Federation; Professor, Deputy Head of the Department; Doctor of Technical Sciences; neurocomputer@yandex.ru

Sychev Artem Konstantinovich , Scientific researcher LLC "SmartTek",Moscow, Russia, Koshtoyantsa str.,21, of. 8; sychev_a_k@mail.ru

***Abstract*—**Based on logically probabilistic approach, we propose a Risk Model for successful attacks on social media on the Internet in terms of information warfare. We formulate and investigate risk-criteria for the decision-making framework aiming to achieve the goals of information warfare. We, finally, propose an algorithmic foundation based on the established criteria for the Hadoop cluster.

Keywords: information warfare, polynomial, risk-models, risk-criteria, actor, social network, monitoring, security function, Hadoop cluster, daemon

1. Introduction

"The Information Warfare within the Internet" is the rivalry among political actors through the use of specialized IT (Information Technology) resources in order to influence the informational space of your opponent, to make an impact on its audience and different spheres of political and power relations in order to establish control over the sources of virtual and electronic policy, Resources actor-opponent and achieve information superiority. In other words, the actor aggressor for information superiority over-actor advocate making information attack against an object in the web-space, whose success is a victory, in the sense of achievement of information superiority.

In fact, citizens become an extensive network of ground-based social touch, reflecting the structure of society in real time in nearly every corner of the world, and the speed and volume of the sensor network, especially in terms of "Internet everywhere" is growing every day.

Hidden information and psychological impact on the population in social networks used to solve the following problems: informational influence on individuals, social and other groups, society as a whole; informational influence on the feasibility and efficiency of administrative decisions by the government and law enforcement agencies adopted on the basis of this information; manipulation of public opinion through the mass media and, in particular, through social networking services; discrediting the leaders of objectionable; automated information dissemination in the major social networks and the organization of information support activities for prepared exposure scenarios and given a mass audience of social networks.

A. Risk models of information influence and destabilizing factors

The model makes it possible to influence the information to study the dependence of the behavior of the subject of his awareness and, consequently, on the impact of information. Having a model of informational influence can pose and solve the problem of synthesis of information management - what should be the impact of information (in terms of the control of the subject), managed to get on the subject of the desired behavior. Finally, unable to solve the problem of

information management, information warfare can be modeled by simulating the interaction of several actors, who have common interests in certain information, and the effect on the managed object. If the model of informational influence (social impact in terms of sociology and social psychology) has been the subject of numerous studies for over half a century, the issues of mathematical modeling is information management and information confrontation in social networks almost never investigated, due to the recent emergence of these.

Based on the above, it can be concluded about the relevance of studying the problem of social networks in terms of improved security of its members by building risk models of information and psychological warfare for the users of social networking.

2. Risk-attack models

A. The applicability of logically probabilistic approach for the integrated risk assessment

Risk Y - an object social media are being attacked by the intruder, consists of two components [1,2]:

- The probability of failure of a counter attack against him (the failure of the object Y) or the probability of a successful attack

- Evaluation (e.g., financial, material, time to repair the damage, etc.) scale consequences (damage) of a successful attack.

The object of risk is considered to be sufficiently protected if given the opportunity to overcome potential barriers probability of a successful attack (the probability of the risk, the probability of failure or vulnerability of the object of risk) $P_A^Y = \left(1 - P_З^Y\right)$than minimum value $P_{A-ДОП}^Y$, i.e.,

$$P_З^Y \geq 1 - P_{A-ДОП}^Y \text{-} \qquad (1)$$

- the condition of the feasibility, where $P_З^Y$ - the probability of a successful counter attack (immunity, the success of the object of risk) subject to risk.

For any object risk Y of [1,3], in general case, there is a complete system of (list) security functions or attributes, each of which is in Table 1 denoted by the binary logic variable X with the appropriate subscript.

Table 1. Security Functions

Security Function	Meaning of Security Function
X_1	Preventing the occurrence of conditions leading to the generation of (occurrence) destabilizing factors (DF)
X_2	Warning immediate manifestations of destabilizing factors
X_3	Detecting manifested destabilizing factors
X_4	Prevention of exposure to risk in the manifested and revealed destabilizing factors
X_5	Prevention of exposure to risk on the manifest, but the undetected destabilizing factors
X_6	Detecting the impact of destabilizing factors on the subject of risk
X_7	Localization (restriction) found the impact of destabilizing factors on the subject of risk
X_8	Localization of undetected exposure to risk by destabilizing factors
X_9	Dealing with the consequences of the localized impact of the detected object on the destabilizing factors risk
X_{10}	Dealing with the consequences of undetected localized exposure to risk by destabilizing factors

The result of each security function, or the outcome is a random event and can take two values - success or failure. It is assumed that a binary logical variable X_j, $j = 1 \div n, n = 10$ is equal to 1 with probability P_j if the execution of the $j-$ security function has led to the failure risk of the object Y, and this binary logical variable equals to 0 with a probability $Q_j = 1 - P_j$, otherwise. The barriers, that are created to counteract the negative effects of destabilizing factors on the subject of risk, are to perform certain security functions that prevent the execution of the attacks on the subject of risk. At the same time, technology, one barrier can consistently perform multiple security functions. Obstruction may perform the security functions against different objects risk.

In general, the logic function (L-function) is the success of the attack, realizing the impact of destabilizing factors as [1,3]

$$Y = Y(X_1,\ldots,X_n),$$

and the probability function (P-function, P-polynomial) is the risk of failure of the object –

$$P(Y = 1/X_1,\ldots,X_n) = \Psi(P_1,\ldots,P_n) = PY .$$

According to the general case of [1,3] L-function (L-polynomial) of the success of an attack is a type of

$$Y = X_1X_2\left(\overline{X_3}X_4 \vee X_3X_5\right)\left(\overline{X_6X_7}X_9 \vee X_6\overline{X_8}X_{10} \vee \overline{X_6}X_7 \vee X_6X_8\right) \qquad (2)$$

and the probability of success of an attack can be calculated using the B-polynomial

$$PY = PY(P_1,P_2,\ldots,P_{10}) = P_1P_2[(1-P_3)P_4 + P_3P_5][(1-P_6)(1-P_7)P_9 + P_6(1-P_8)P_{10} +$$

$$+(1-P_6)P_7 + P_6P_8] \ . \qquad (3)$$

Destabilizing Factors (DF) for social networks, of course, have their own specifics. DFs appear in text messages, in the network structure of society, and other places. To assess the socio-economic system, DFs use markers of social stress - stress quantitative active Internet users.

B. Social markers

There are 6 types of markers [4]:

1. Markers activity. The values are calculated by direct marker of counting the number of messages and users per unit time. Higher values of these markers indicate an increased activity in a certain period of time; mass reaction to some event or "stuffing" of information.

2. Psycholinguistic markers. Display the emotional state of the author's text message. The massive increase in the indicators of emotional stress indicates the emotional contamination - the grouping process on the basis of common passion.

3. Lexical tokens. Analysis is carried out using tone text messages (words denoting negative emotional states; words with destructive semantics).

4. Semantic markers. Simple/easily distinguishable meanings, for example: destructive, directive, liquidators, results.

5. Network markers. In the process of dissemination of information among people there is a greater number of connections with like-minded people. Normally the graph model satisfies users "small world." Thus, the marker is an integral indicator of the following parameters of the graph: the diameter of the graph; the average coefficient of mediation, clustering; the density of the graph; connectivity, and others.

6. Markers consumption. Is an integral indicator that takes into account intra-regional studies of the following indicators: number of calls, average call duration, size, frequency, and the total amount of airtime purchases.

The causal completeness of [1] security functions is an important property of logically probabilistic approach. At the same time, within the framework of refinement and specification information in the context of the attack on the object based on the risk characteristics of the social markers and information warfare practices for each of the security functions that are introduced graduation security functions.

C. New graduation security functions based on social markers

By analogy with the foregoing, we assume that the binary logical variable $X_j,\ j=1\div n,\ n=10$ corresponding to r-th gradation of j-th security function is 1 with probability P_{jr}, if because performing j-th security function has led to a failure. And this X_j equals to 0 with probability $Q_{jr}=1-P_{jr}$, otherwise. Each group of gradations for X_j is a full group of events $\{X_{jr}\}_{r=1}^{N_j}$, so we can use Bayes' formula [1]

$$P\left(X_{jr}/X_j\right)=\frac{P\left(X_{jr}\right)P\left(X_j/X_{jr}\right)}{\sum_{r=1}^{N_j}P\left(X_{jr}\right)P\left(X_j/X_{jr}\right)}. \qquad (4)$$

Formula (4) can be used for iterative learning (configuration identification) L-B-polynomials (2), (3) on the statistical data to clarify the value of this risk. Thi algorithm can be organized in some rational way, for example as given in [1].

In order to develop constructive solutions, including architecture, circuit design and algorithmic solutions for the automation of the identification of information and counter attacks, it is advisable to extend the functionality, the

introduction of new grades of these security functions, putting them in line with the newly indexed binary logic variables are shown in Table 2.

Table 2. New gradation, extending functionality security functions from information attacks on social media

Security Function	Meaning of Security Functions
X_{11}	Preventing an environment leading to the generation (emergence) of DF exposure to the object itself on the basis of the risk of social markers
X_{12}	Collect information about an attack against object risk Y in social media in some Enterprise Network on the basis of all the information about changes in the social markers
X_{13}	Collect information about an attack in centralized organization, based on all the information it received
X_{31}	Detection of an attack based on information from a centralized organization
X_{32}	Detection of an attack based on information from other Enterprise Networks in the domain
X_{33}	Detection of an attack based on information from other domains
X_{51}	Preventing, through social markers, the exposure to the risk of undetected object DF based on information from other Enterprise Networks in the domain
X_{52}	Preventing, through social markers, the exposure to the risk of undetected object DF based on information from a centralized organization in this domain
X_{53}	Preventing, through social markers, the exposure to the risk of undetected object DF based on information from other domains.

New L-polynomial for social-media must be taken into account new components according to the table. 2, namely:

$$X_1 = X_{11}\overline{X}_{12}\overline{X}_{13} \vee \overline{X}_{11}X_{12}\overline{X}_{13} \vee \overline{X}_{11}\overline{X}_{12}X_{13} \vee X_{11}X_{12}\overline{X}_{13} \vee X_{11}\overline{X}_{12}X_{13} \vee$$

$$\vee \overline{X}_{11}X_{12}X_{13} \vee X_{11}X_{12}X_{13},$$

$$X_3 = X_{31}\overline{X}_{32}\overline{X}_{33} \vee \overline{X}_{31}X_{32}\overline{X}_{33} \vee \overline{X}_{31}\overline{X}_{32}X_{33} \vee X_{31}X_{32}\overline{X}_{33} \vee$$

$$\vee X_{31}\overline{X}_{32}X_{33} \vee \overline{X}_{31}X_{32}X_{33} \vee X_{31}X_{32}X_{33},$$

$$X_5 = X_{51}\overline{X}_{52}\overline{X}_{53} \vee \overline{X}_{51}X_{52}\overline{X}_{53} \vee \overline{X}_{51}\overline{X}_{52}X_{53} \vee X_{51}X_{52}\overline{X}_{53} \vee$$

$$\vee X_{51}\overline{X}_{52}X_{53} \vee \overline{X}_{51}X_{52}X_{53} \vee X_{51}X_{52}X_{53}.$$

Substituting the obtained logical expressions in (2) we obtain the L-function of the success of an attack in social-media.

Similar to the previous theoretical results, it can be generated/generalized for each specific gradation of 6 social markers. Thus the analytical expressions for the L-function and B-polynomial information attack can be easily, methodically, refined with new knowledge, including intelligence on new DF, influencing the behavior of social markers for specific cases of information warfare. The power of the set of security functions is increasing.

3. Risk assesment criteria of protected object of information warfare. Price risk

From (2) logical condition for the failure of an attack (L-criteria) can be written as follows:

$$Y_A = 0,$$

is satisfied if at least one of the conditions below is satisfied:

$$\begin{cases} X_1X_2 = 0, \\ \overline{X_3}X_4 \vee X_3X_5 = 0, \\ \overline{X_6X_7}X_9 \vee X_6\overline{X_8}X_{10} \vee \overline{X_6}X_7 \vee X_6X_8 = 0. \end{cases}$$

According to (3), the failure of information attack probability condition (P-criteria) can be written as follows:

$$PY = 0,$$

is satisfied if at least one of the conditions below is satisfied:

$$\begin{cases} P_1 P_2 = 0, \\ (1-P_3)P_4 + P_3 P_5 = 0, \\ (1-P_6)(1-P_7)P_9 + P_6(1-P_8)P_{10} + (1-P_6)P_7 + P_6 P_8 = 0. \end{cases}$$

In general, the ratio of the calculated values of L-function and B-polynomial allows us to estimate the action actor aggressor, attacking an object in social-media on the basis of information from the intelligence, using protecting barriers, peculiarities of the security functions, as well as the existing vulnerabilities in them. Technically, it would be written as actor aggressor known model (2) and (3) with security functions $X_1^A \div X_n^A$ and the probability of failure $P_1^A \div P_n^A$. As the allowable probability of failure, risk object (see (1)) can take the value calculated by (3), in the probabilities of failure $P_1^A \div P_n^A$. For actor-aggressor assessment of security risk to the value of the object is $1-P_{A-ДОП}^Y$. Then the value of the difference is defined as [1]

$$\Delta = P_3^Y - \left(1-P_{A-ДОП}^Y\right), \qquad (5)$$

where the value of P_3^Y calculated by the formula (3), characterized by the implementation of the objective conditions of the reachability (1) and the quality of "armor" barriers, implementing security functions object risk.

We introduce a new measure

$$\Delta Y = YY_A.$$

From (5) it follows that if at least one of the conditions (criterion of exhaustion of reserve risk the stability of the object)

$$\begin{cases} \Delta < 0, \\ \Delta F = 1, \end{cases}$$

There is an evidence to urgently strengthen the security of the object of risk.

If at least one of the conditions is carried out (a criterion of the presence of the stability margin of the object of risk)

$$\begin{cases} \Delta \geq 0, \\ \Delta F = 0, \end{cases}$$

it indicates the presence of the stability margin of the object to the risk of attacks by actor aggressor. Accordingly, it is necessary that an actor aggressor invests additional resources in improving the attack on the object of risk.

Cost of risk can be estimated by the following formula

$$CY = \begin{cases} CY_{ДОП}\text{ , when } \Delta \geq 0 \text{ or } \Delta Y = 0\text{ ,} \\ CY_{ДОП} + C\text{ , when } \Delta < 0 \text{ or } \Delta Y = 1\text{ ,} \end{cases}$$

where $CY_{ДОП}$ - the cost of acceptable risk, C - a term that depends on many factors specific to information warfare, the choice of values which is an separate problem on its own.

4. Cluster information warfare among Hadoop

The authors, in a team, are doing research trying to automate the information counter attacks in social media. Methodological approaches to the creation of algorithms and software solutions in the environment of web-programming, Hadoop, for a wide class of problems of monitoring sites in the web-space. Designed cluster topology Monitoring Hadoop, having common application [5]. The research and the algorithm measuring attributes of monitoring facilities in the web-space to meet the requirements of unity of measurements. On the basis of neuro-fuzzy approaches, we developed recommendations following the creation of technological procedures - Assessment of the object of monitoring and identification of its information model. We also formulated system requirements for the design of the monitoring cluster Hadoop [5].

According to the creators of such monitoring, cluster must have its functionality required for the functioning of the fullness of the control system (CS) Social Media (SM). In other words CS should receive from it all the necessary information to make decisions. Technologically, Hadoop cluster management system module (Fig. 1) can be represented as two daemons - **DataNode_Social_Media** responsible for the formation of information model of attacks on social media and **TaskTraker_Social_Media** daemon responsible for the control actions to restrain the attacks on social media. Then the proposed new cluster topology information warfare among Hadoop, is schematically illustrated in Fig. 1.

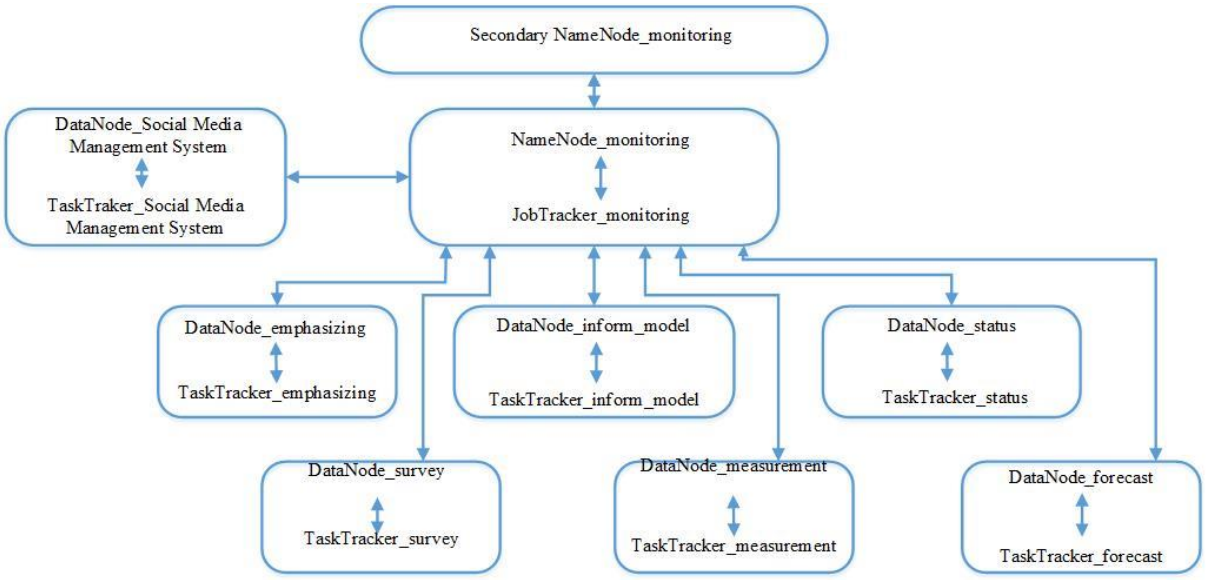

Figure 1. Cluster Topology information warfare among Hadoop. Description daemons are given in [5].

The ability to reliably predict, on the basis of SM, such events as upcoming social unrest, ranging from riots and protests and ending assassinations and coups, enables timely decisions to prevent such disasters, without waiting for the tragic conflict, eventually contributing to the stability, peace and order in individual countries, regions and globally.

It can be concluded that the forecast of the actual behavior of a certain scenario social networking in the future. This objective can be accomplished by the construction and study of high-quality models of complex social and economic systems, including social, political, economic, informational and other factors. The result is a set of modeling scenarios of the social network, depending on the state of its information infrastructure, and by environmental factors. In addition, the ultimate goal of simulation is to develop recommendations for the development of effective in terms of achieving a given set of objectives and performance criteria of control actions.

A. Synthesis of new daemons

On the basis of the above, the following guidelines designing software modules ***DataNode_Social_Media*** and ***TaskTraker_Social_Media*** daemons in the form of the following sequence of steps.

1. Define a monitoring object. Formation of its information models in a software module into a daemon ***DataNode_Social_Media***.

2. Create a complete set of security functions and their grades in a software module ***DataNode_Social_Media*** daemon.

3. Develop software modules that implement the L-polynomial and B-polynomial into a daemon ***TaskTraker_Social_Media***.

4. Develop software modules for risk assessment criteria of a protected object of information warfare in the daemon ***TaskTraker_Social_Media***.

5. Develop software modules into a daemon ***TaskTraker_Social_Media*** for calculating the price risk of the object of information warfare.

6. Develop software modules into a daemon ***TaskTraker_Social_Media*** to take decisions on further actions based on the results in steps 4 an 5.

7. Set-up Hadoop-cluster information warfare.

Decisions points 1-6 are specified in the operation of the cluster of information warfare as new knowledge of the security functions and algorithms underlying the above-mentioned software modules and daemons ***DataNode_Social_Media*** and ***TaskTraker_Social_Media***. This is done continuously updated software modules other daemons that cluster.

5.Conclusion

As the scientific and methodological framework is proposed to use the formalism of logically probabilistic approach, allowing the model to information attacks social-media risk positions. This approach is flexible, based on the new knowledge to clarify the actions of the attacker, which makes it relatively easy to specify, develop models of risk of attack.

To evaluate the DF socio-economic systemы used markers of social stress - stress quantitative active Internet users. Proposed a risk-based model of social stress markers.

Developed risk assessment criteria of a protected object of information warfare.

For the proposed cluster topology information warfare among Hadoop, we developed guidelines synthesis algorithmic bases, program modules and daemons ***DataNode_ Social_Media*** and ***TaskTraker_ Social_Media.***

References

Article in a journal:

[1] A. N. Nazarov, “Estimation of information safety level of modern infocommunication networks on basis of logic-probability approach,” Automation and Remote Control, July 2007, Volume 68 Issue 7, 2007, pp. 1165-1176, doi: 10.1134/S0005117907070053.

[2] A. N. Nazarov, “LOGICAL-AND-PROBABILISTIC MODEL FOR ESTIMATING THE LEVEL OF INFORMATION SECURITY OF MODERN INFORMATION AND COMMUNICATION NETWORKS,” Telecommunications and Radio Engineering, USA, 2010, Vol. 69, № 16, pp. 1453-1463, doi: 10.1615/TelecomRadEng.v**69**.i**16**.60.

Article in a conference proceedings:

[3] Nazarov A. ‘Botnet tracking and global threat intelligence - behavior approaches to identifying distributed botnets‘ paper presented at the IEEE / Collection of proceedings of the *Cybersecurity Summit (WCS), 2012 Third Worldwide, New Dehli, 30-31 Oct. 2012.* http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6780878&newsearch=true&queryText=Botnet%20tracking%20and%20global%20threat%20intelligence%20-%20behavior%20approaches%20to%20identifying%20distributed%20botnets

[4] Osipov G.S. Methods and software for assessments of social stress, based on analysis of information online. Access: https://www.gkpromtech.ru/material/view?id=27. Date of circulation: 02.10.2015.

[5] Volkov, D., Nazarov, A. & Nazarov, M 2014, ′A global threat - the dark web′, paper presented in the annual Collection of scientific works of International conference Managing the development of large-scale systems" (MLSD'2014), Institute of control Sciences RAS, pp. 452-459.